

Eingebettete Systeme

- Bluetooth -

Lothar Thiele, Jan Beutel

Übersicht

• Einleitung	1
• Architektur	10
• Pakete und Kanäle	25
• Modi, Zustände und Verbindungsaufbau	36
• Implementierung	46

Die Folien enthalten Material der Firma Ericsson.

Anwendungsszenarien

- Kabelersatz (Drucker, PC, Personal Digital Assistant, Maus, Keyboard)
- Automatische Synchronisation zwischen PC und PDA, Telefon, elektronische Postkarte, elektronische Visitenkarte
- Austausch von Informationen in einem Konferenzszenario
- Hausautomatisierung, Entertainment
- Industrielle Steuerung, Sensoren, Aktoren
- Zugangskontrolle
- Computer zum Anziehen ...
- Drahtlose Kopfhörer-Mikrofon-Display-Kombination (Headset)
- ...

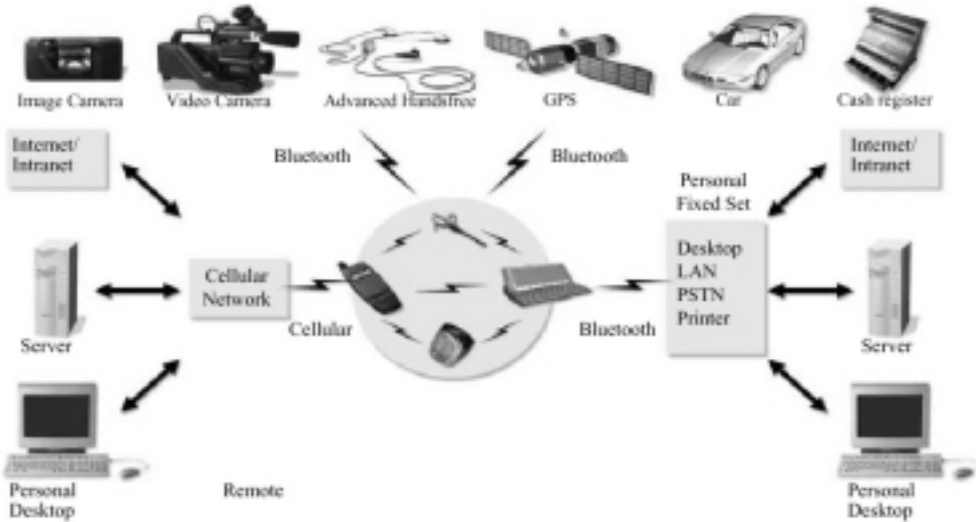
Anwendungsszenarien

The Distributed Approach to Information Processing



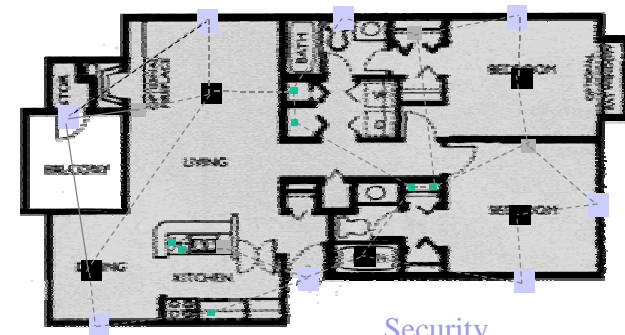
Source: Richard Newton

Anwendungsszenarien



Anwendungsszenarien

The Obvious Choice - The Smart Home and Network Appliances

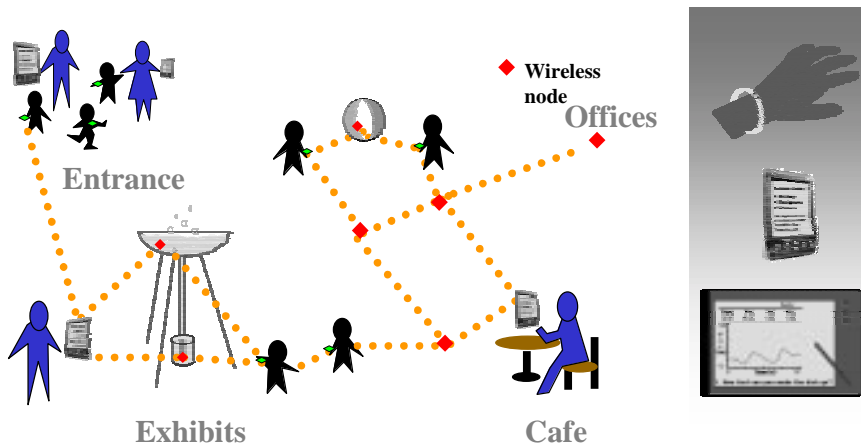


Dense network of sensor and monitor nodes

Security
Environment monitoring and control
Object tagging
Identification

Anwendungsszenarien

Interaktives Museum



Standards für den letzten Meter

- **Bluetooth**
 - Kabelersatz, kurze Reichweite, kleiner Leistungsverbrauch
 - Bandbreite 1 Mbit/s (Erweiterung auf 2Mbit/s geplant)
 - Punkt-zu-Punkt oder Broadcast Verbindung
 - Sendeleistung 1 mW
- **HomeRF**
 - Heimnetzwerk, Konkurrenz zu Wireless LAN
 - Bandbreite bis 10 Mbit/s
 - Zentrale Basisstation notwendig
 - Sendeleistung 100 mW
- **Wireless LAN (IEEE 802.11)**
 - Heim/Firmennetzwerk, Funktionalität vergleichbar mit Ethernet
 - Bandbreite 11 Mbit/s
 - Zentrale Basisstation notwendig
 - Sendeleistung 100 mW (1 W in USA)

Wer war Bluetooth?

- Wikinger
- König von Dänemark 940-981
- Christianisierte, vereinigte und kontrollierte Dänemark und Norwegen



Architektur im Überblick

- **Entwurfsziele**
 - kleine Implementationsgrösse (1 cm²)
 - kleine Kosten (5\$)
 - kleiner Leistungsverbrauch (mW)
 - sichere Übertragung (Verschlüsselung, Authentifikation)
 - robuste Übertragung (Interferenz mit Wireless LAN, Mikrowellengeräten und HomeRF)
 - Flexibilität in der Hardware-Software Implementierung
- **Technische Daten**
 - 2.4 GHz Band (international freigegeben, spektrale Bandbreite 79 MHz, Frequenzsprungverfahren und Zeitmultiplex)
 - 10-100 m Übertragungsbereich
 - maximal 1 Mbit/s Bandbreite für eine Verbindung
 - gleichzeitige Übertragung von Sprache-Video (synchron, isochron) und Daten (asynchron)

Architektur im Überblick

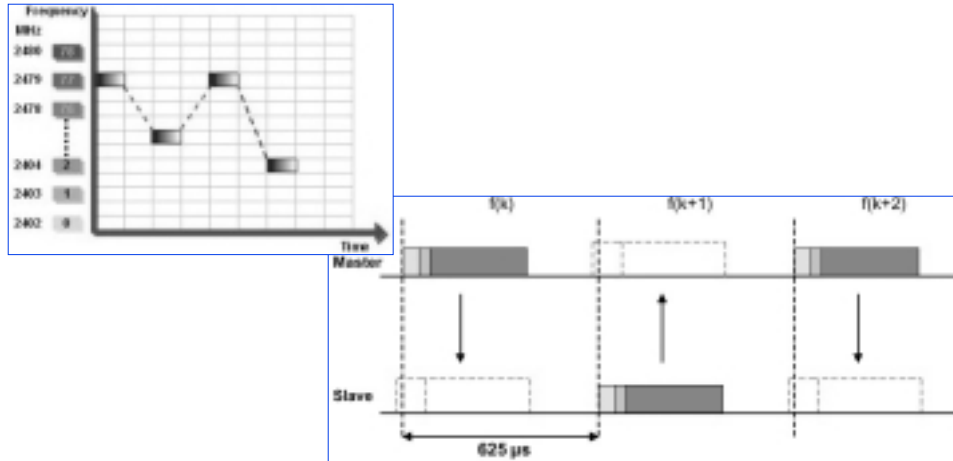
- **Spezialitäten**
 - flexible Gerätemodi und Gerätezustände (aktiv, hold, sniff, park, stand-by, scan, page, inquiry)
 - adaptive Sendeleistung zur Reduktion des Leistungsverbrauchs
 - synchrone (z.B. Sprache) und asynchrone Datenübertragung
 - ad hoc Netzwerk (spontaner Verbindungsaufbau und -abbau, dynamische Netzwerktopologie, keine zentralisierte Koordination)
 - flexible Netzwerktopologien (Piconet, Scatternet)
 - Entdecken von Dienstleistungen (service discovery)

Architektur im Überblick

- **Frequenzsprungverfahren**
 - Sender springt von einer Frequenz zur anderen mit einer spezifizierten Rate (1600 Wechsel/s). Die Reihenfolge (Kanalsequenz) wird nach einer Pseudozufallssequenz der Länge $2^{27}-1$ bestimmt.
 - Frequenzbereich (2402 + k) MHz, k = 0 ...78 .
 - Die Datenverbindung also in Zeitfenster der Länge 0.625 ms aufgeteilt; jedes Zeitfenster bzw. Paket wird auf einer anderen Frequenz übermittelt.

Architektur im Überblick

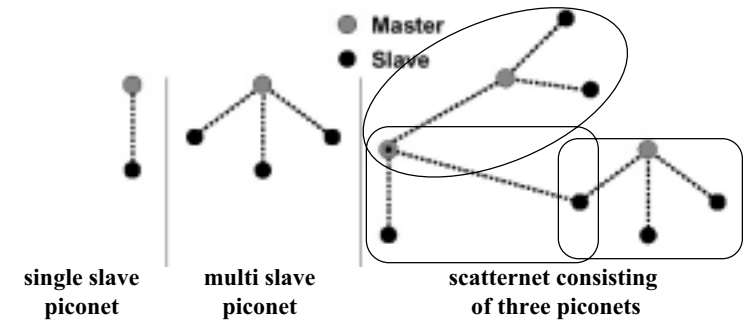
● Beispiel zum Frequenzsprungverfahren:



Netzwerktopologien

● Mobile Topologie

- alle Geräte sind potentiell mobil
- dynamischer Verbindungsaufbau
- hierarchischer Verbund mobiler Teilnetze



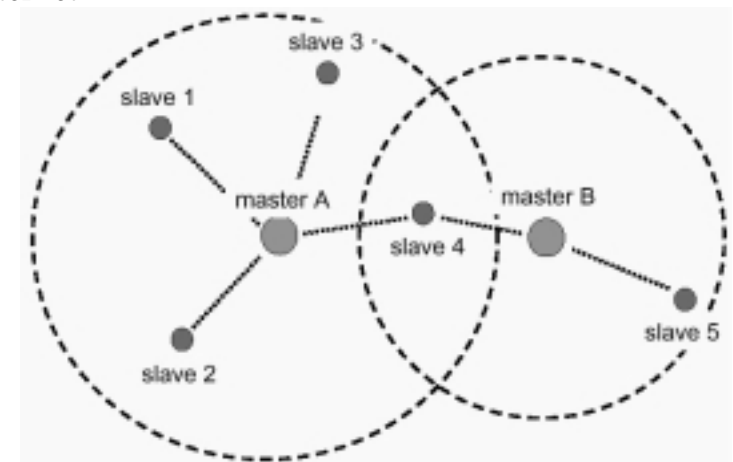
Netzwerktopologien

● Piconetz

- Ein Piconetz besteht aus 1 Master und bis zu 7 Slaves.
- Alle Geräte in einem Piconetz benutzen die Kanalsequenz (bestimmt durch die Device-Adresse des Masters BD_ADDR) und Phase (bestimmt durch Systemtakt des Masters) des Masters ; Master und Slaves teilen sich also einen Kanal.
- Verbindungen sind entweder zwischen Master und einem Slave (Punkt-zu-Punkt) oder Master und allen Slaves.
- Auf einem Kanal sind folgende Verbindungen möglich:
 - » 432 kBit/s (duplex) oder 721/56 kBit/s (asymmetrisch) oder
 - » 3 gleichzeitige Sprachkanäle pro Piconetz oder
 - » eine Kombination von Daten und Sprache.

Netzwerktopologien

● Scatternetz

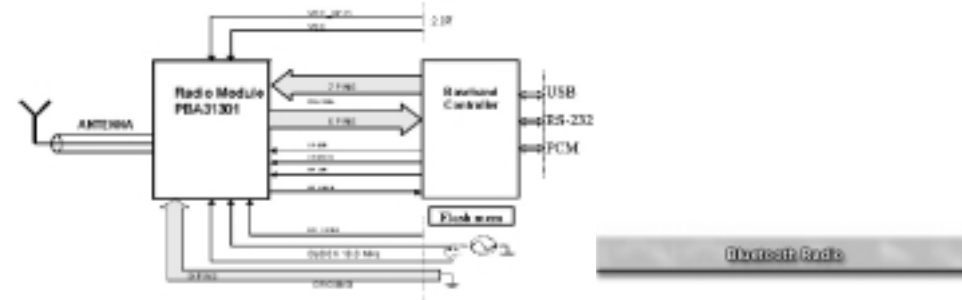


Netzwerktopologien

- **Scatternetz**
 - Mehrere Piconetze mit überlappenden Geräten formen ein Scatternetz.
 - Slaves können in mehreren Piconetzen enthalten sein; ein Modul kann Slave in verschiedenen Piconetzen sein, Master aber nur in einem.
 - Die Kanalsequenzen der beteiligten Piconetze sind nicht synchronisiert. Zur Datenübertragung zwischen Piconetzen selektiert der Slave den entsprechenden Master, passt seine Kanalsequenz und Phase entsprechend an und synchronisiert sich damit mit dem Kanal des Piconetzes.

Protokollhierarchie

- Die **Radio** Spezifikation definiert die Frequenzbänder, die Sender- und die Empfängereigenschaften und stellt somit die Kompatibilität zwischen den Transceivern sicher.



Protokollhierarchie

- Die **Baseband**-Spezifikation definiert die Paketformate, die physikalischen und logischen Kanäle, die Fehlerkorrektur, die Synchronisation zwischen Sender und Empfänger, die unterschiedlichen Operationsmodi und Zustände, die den Daten- und Sprachtransport ermöglichen.
- Die **Audio**-Spezifikation definiert die Sprachübertragung, speziell die Kodierung und Dekodierung.
- Der **Link Manager** (LM) behandelt die Authentifizierung einer Verbindung und die Verschlüsselung, das Management eines Piconetzes (synchrone/asynchrone Verbindung, Steuerung der Übertragungsqualität), das Aufsetzen einer Verbindung (asynchrone/synchrone Pakettypen, Namen/ID-Austausch) und die Zustands- und Moduswechsel eines Gerätes.



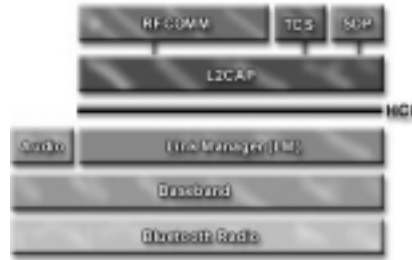
Protokollhierarchie

- Das **Host Controller Interface** (HCI) liefert eine gemeinsame standardisierte Schnittstelle zwischen einem Host und einem Bluetooth Gerät, spezifiziert für verschiedene Schnittstellen (USB, RS232, PCI, ...).
- Das **Link Layer Control and Adaptation Layer Protocol** (L2CAP) bietet eine abstrakte Schnittstelle für die Datenkommunikation. Es segmentiert Pakete (bis 64kByte) und fügt sie wieder zusammen, ermöglicht das Multiplexen von Verbindungen (gleichzeitige Benutzung mehrere Protokolle und Verbindungen) und erlaubt den Austausch von Qualitätsinformationen zwischen zwei Geräten (Paketrate, Paketgröße, Latenz, Delayvariation, maximale Rate).



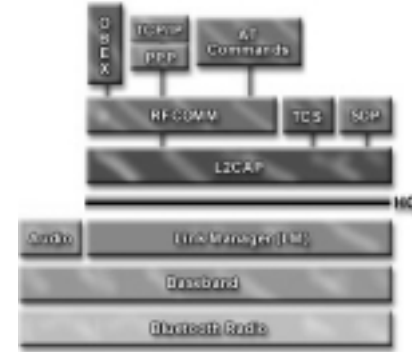
Protokollhierarchie

- **RFCOMM** ist ein einfaches Transportprotokoll, das eine serielle Schnittstelle emuliert (~RS 232).
- Die **Telephony Control protocol Specification (TCS)** ermöglicht die Signalisierung für die Herstellung und Unterhaltung von Daten- und Sprachverbindungen (Terminal, Gateway, Lautstärke, auflegen-abheben, ...).
- Das **Service Discovery Protocol (SDP)** erlaubt es Anwendungen, die Dienste und Eigenschaften andere Bluetooth-Geräte zu erkennen. Diese Dienste können dann durch andere Protokolle genutzt werden.



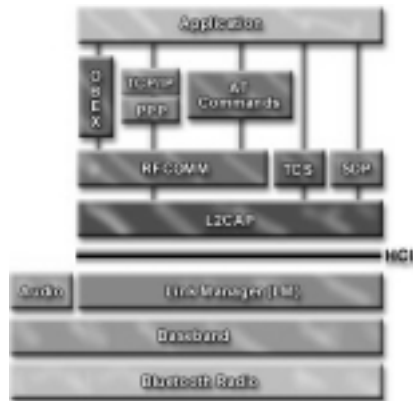
Protokollhierarchie

- Eine Vielzahl von Protokollen sind auf die beschriebenen Basisdienste aufgesetzt.
 - **OBEX (Object Exchange Protocol)** wird zum Filetransfer und zur Datensynchronisation benutzt.
 - **TCP/IP** wird in Internet-Anwendungen eingesetzt.
 - Eine Menge von **AT-Kommandos** ermöglicht die Steuerung über eine Terminal-Verbindung.
 - **WAP ...**

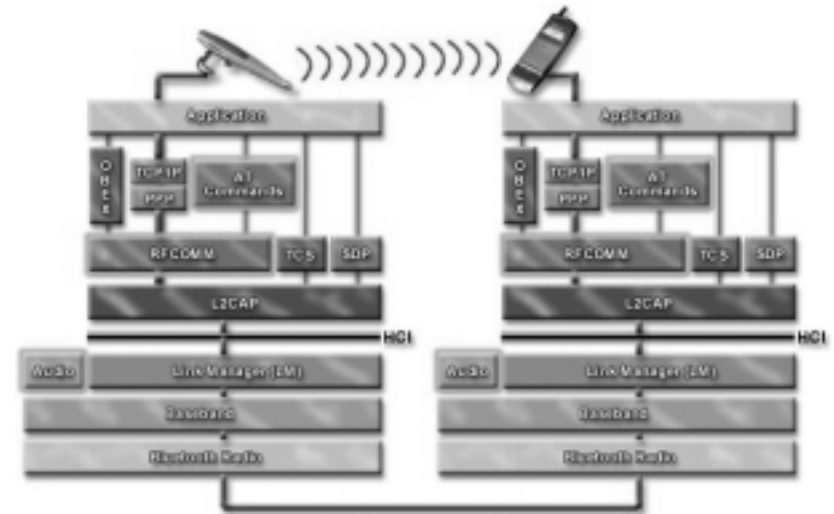


Protokollhierarchie

- Die **Application-Ebene** schliesslich ermöglicht Anwendungen, die eine Kommunikation über Bluetooth einsetzen. Sie greift auf die Dienste der unteren Protokollebenen zu.



Protokollhierarchie



Addressierung

- **Bluetooth Geräte Adresse BD_ADDR**
 - 48 Bit breit
 - IEEE 802 kompatibel (Ethernet, Token Ring, Wavelan)
 - Eindeutige Adresse für jedes Gerät.
- **Active Member Adresse AM_ADDR**
 - 3 Bit für maximal 7 aktive Slaves in einem Piconetz.
 - Adresse "Null" wird als Broadcast an alle Slaves interpretiert.
- **Parked Member Adresse PM_ADDR**
 - 8 Bit für parkierte Slaves.

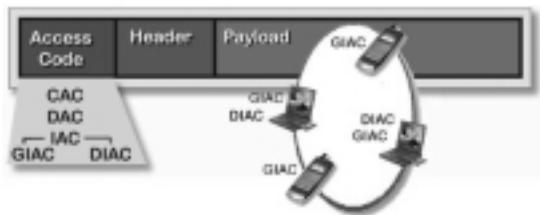
Paket Format



- Access Code** Identifiziert alle Pakete die zwischen Bluetooth-Geräten ausgetauscht werden.
- Packet Header** Verbindungskontrolle zwischen Master und Slave.
- Payload** Nutzdaten.

Access Code

- Der Access Code ist abhängig vom Betriebsmodus, z.B. Verbindungsmodus, Pagemodus, Inquirymodus.



- **Channel Access Code** Identifiziert alle Pakete, die auf einem physikalischen Kanal (Piconetz) ausgetauscht werden.
- **Device Access Code** Wird im Pagemodus benutzt.
- **Inquiry Access Code** Wird bei der Serviceerkennung benutzt.

Paket Header Format



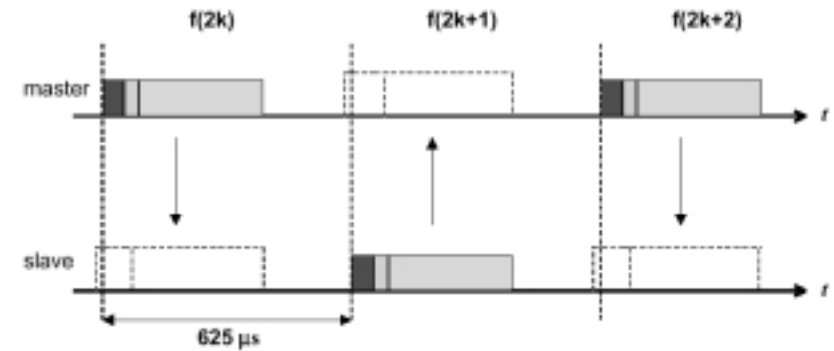
parameter	information
AM_ADDR	slave active member address
TYPE	payload type
FLOW	LC flow control
ARQN	ACK/NAK
SEQN	retransmit ordering
HEC	header error check

Verbindungstypen

- Gemischte Übertragung von **Daten und Sprache**
- Synchronous Connection-Oriented (**SCO**) Verbindung
 - Symmetrischer, synchroner Service.
 - Slotreservierung zur Paketübertragung in regelmässigen Intervallen.
- Asynchronous Connection-Less (**ACL**) Verbindung
 - (A)symmetrischer, asynchroner Service.
 - Keine Slotreservierung.
 - Der Master sendet spontan, der angesprochene Slave antwortet im darauffolgenden Slot.

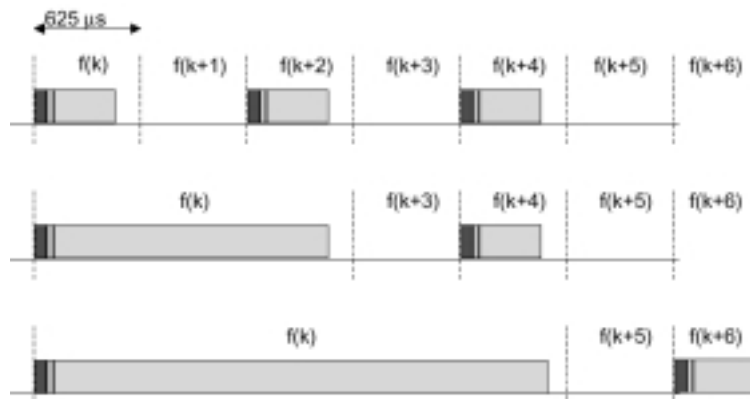
Frequenzsprung Zeitmultiplex

- Auf ein Paket des Masters folgt unbedingt ein Paket des Slave.
- Nach jedem Paket wird der Kanal (Frequenz) gewechselt.

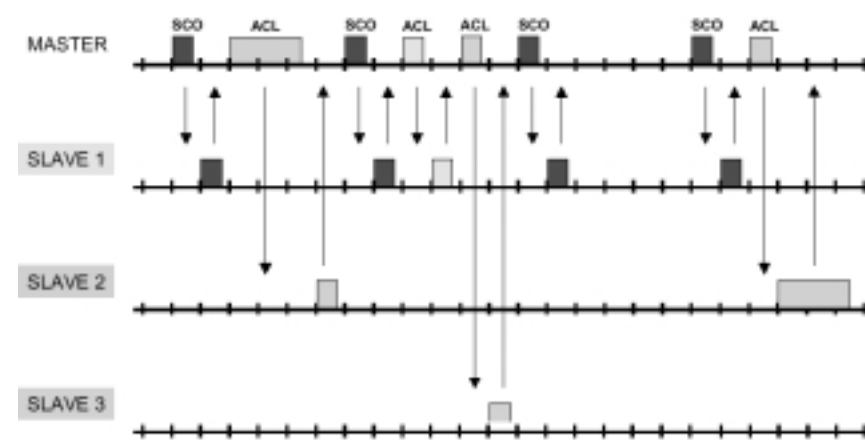


Multi-Slot Pakete

- Asynchroner Datenverkehr, 2x 432.6 oder 723/57.6 kbit/s



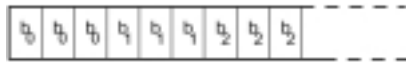
ACL und SCO Verbindungen



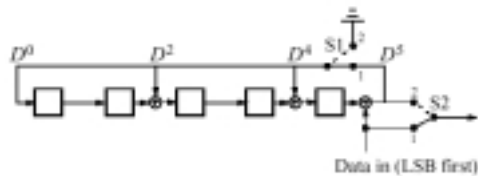
Fehlerkorrektur

- Vorwärtsgerichtete Fehlerkorrektur (FEC).
- Ziel ist es die Paketwiederholungen zu reduzieren; dadurch ergibt sich jedoch ein grosser Zusatzaufwand auch bei guten Kanalbedingungen.

- 1/3 rate: **Bit Wiederholungssequenz** für Header



- 2/3 rate: (15,10) **Hamming Sequenz** für Daten

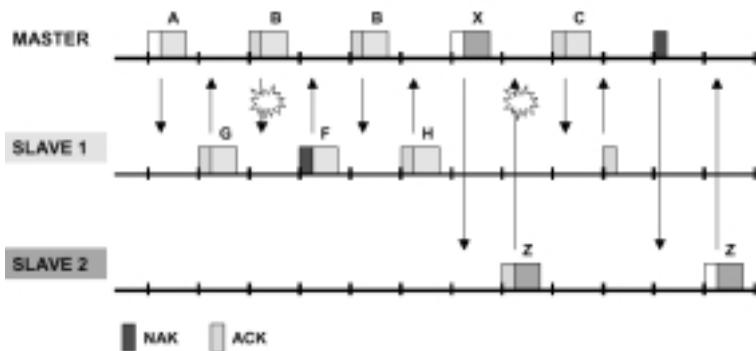


Fehlerkorrektur Paketwiederholungen

- **Automatic Repeat reQuest**

- Steuerung durch das ARQN-Feld im Header des Paketes: ACK/NAK AcKnowledge/Not AcKnowledge
- 1 Bit Sequenznummern SEQN im Paketheader um Paketwiederholungen bei einem verlorenen ACK am Empfänger zu erkennen.
- Integriert in den Header des Antwortpaketes, d.h. es gibt kein spezielles Acknowledge-Paket.

ARQ - Automatic Repeat reQuest



- Not AcKnowledge → erneutes Senden von Paket B
- AcKnowledge → erneutes Senden von Paket Z

Modi und Zustände

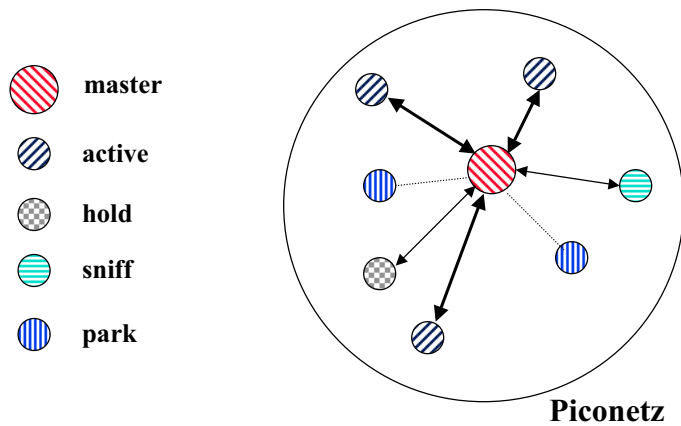
- **Betriebsmodi:**

- **Verbindung** (Verbindung zwischen Master und Slave ist etabliert)
- **Page** (Master stellt Verbindung zu Slave her, dessen Adresse BD_ADDR bekannt ist)
- **Inquiry** (Master besorgt sich Adressen benachbarter Slaves)

- **Zustände im Verbindungsmodus** (sortiert nach sinkendem Leistungsverbrauch)

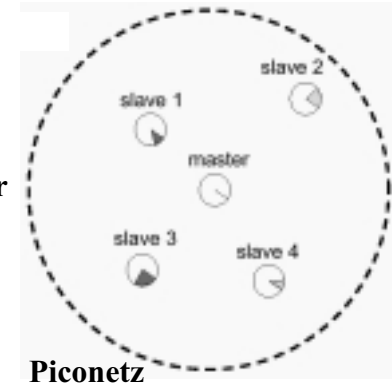
- **active** (aktiv in einer Verbindung zum Master)
- **hold** (verarbeitet keine Datenpakete)
- **sniff** (wacht in regelmässigen Zeitabständen auf)
- **park** (passiv, in keiner Verbindung zum Master, noch synchronisiert)

Zustände im Verbindungsmodus

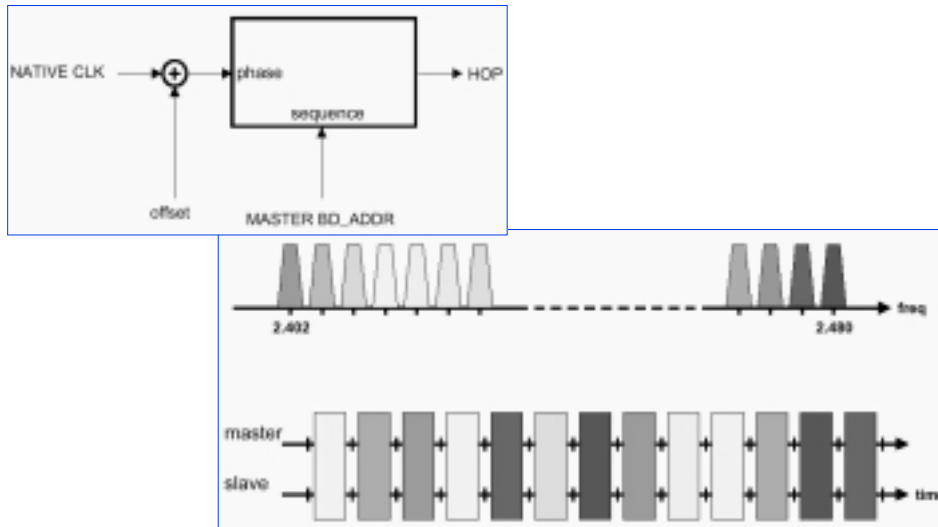


Synchronisation im Verbindungsmodus

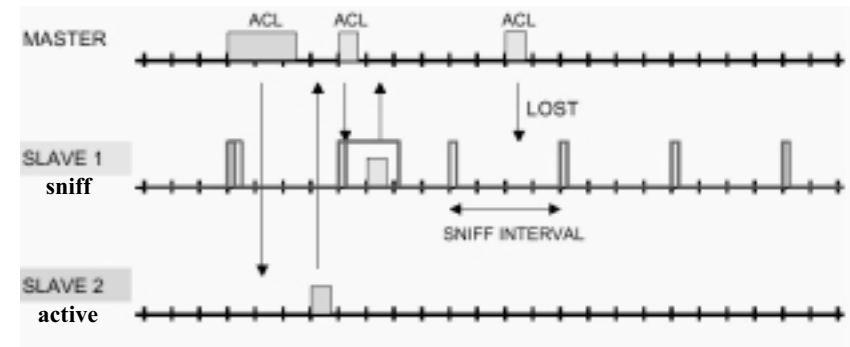
- Die **Kanalsequenz** des Piconetzes wird durch die **BD_ADDR** des Masters bestimmt.
- Die **Phase** innerhalb der Sequenz wird durch den Master bestimmt; alle Slaves richten sich danach.



Synchronisation im Verbindungsmodus



Der Sniff-Zustand

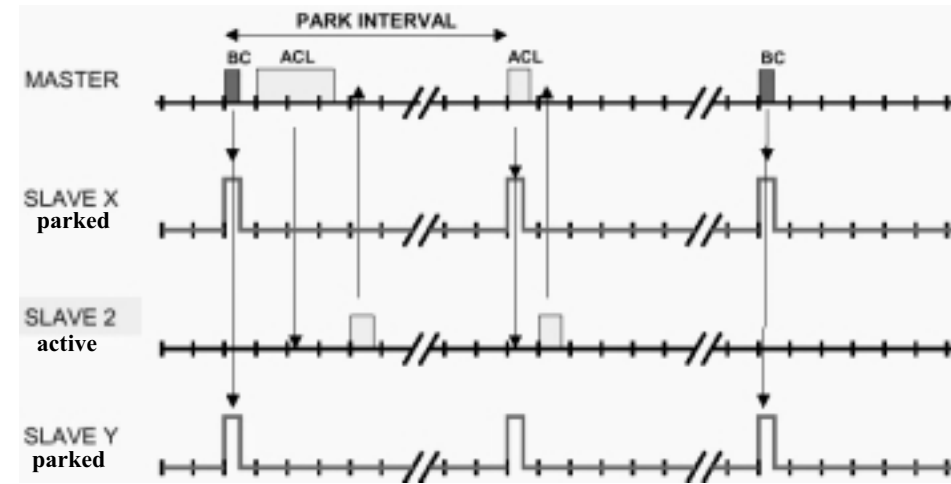


Ein Slave im Sniff-Modus hört in regelmässigen Intervallen, ob ein Paket mit seiner Adresse gesendet wird. Falls ja, antwortet er dem Master

Der Park-Zustand

- Ein Slave im **Park-Modus** nimmt nicht aktiv am entsprechenden Piconetz teil. Ihm ist keine (der 7) Active Member Adressen (AM_ADDR) zugeordnet sondern eine Parked Member Adresse (PM_ADDR).
- Der Master benutzt bestimmte Zeitabschnitte (**Parkintervall**), um mit den parkierten Slaves mittels spezieller Pakete (Beacons BC) zu kommunizieren. Falls diese Paket die PM_ADDR eines parkierten Slaves enthalten, wechselt dieser in den aktiven Modus.
- Die parkierten Slaves nutzen die im Parkintervall gesendeten Pakete zur **Synchronisation**.

Der Park-Zustand



Der Page-Modus

Synchronisation zwischen Master und Slave.
Voraussetzung für den Aufbau einer Verbindung.

page

Master überträgt Adresse des Slaves (benutzt spezielle Kanalsequenz).

page scan

Slave hört, ob seine Adresse gesendet wird.

master page response

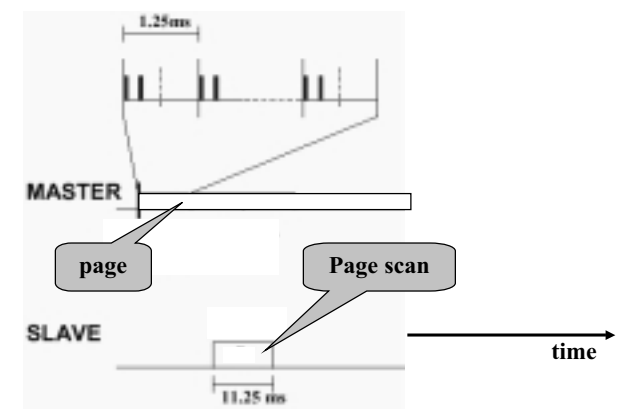
Slave sendet Antwort an den Master (eigene Adresse)

slave page response

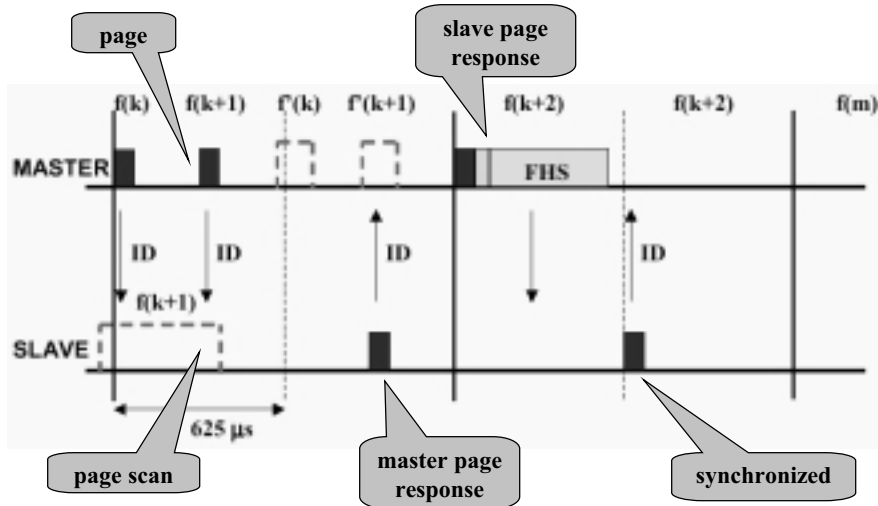
Master sendet FHS-Paket (frequency hop synchronization) an den Slave. Es enthält Kanalsequenz und Phase des Piconetzes.

Problem:
Synchronisation

Der Page-Modus



Der Page-Modus



Hardware-Software-Partitionierung

Evolution

- Radio-Basband-LM in 5 Chips (CPU, RAM, Flash-Speicher, Baseband, Radio), vor 1998
- Radio-Basband-LM in 3 Chips (Link Controller = Baseband+CPU+RAM, Radio, Flash-Speicher), 2000
- Radio-Basband-LM in 2 Chips (Link Controller = Baseband+CPU+RAM+Flash-Speicher, Radio)
- Radio-Basband-LM in 1 Chip
- Alle Protokollebenen in einem "System-on-a-Chip"

Designkriterien

Prozessor

- Rechnerarchitektur sollte breite Datenworte und Operationen auf Teilworten unterstützen.
- Beispiel: 32 bit Mikrokontroller

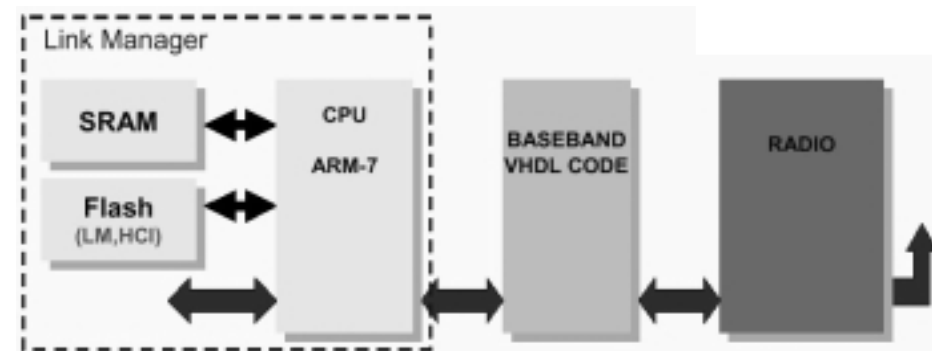
Baseband Timing

- Innerhalb einer halben Paketlänge (321.5 μ s) müssen Pakete verarbeitet werden können.
- Funktionalität der Verbindungssteuerung muss in dieser Zeit abgeschlossen sein.

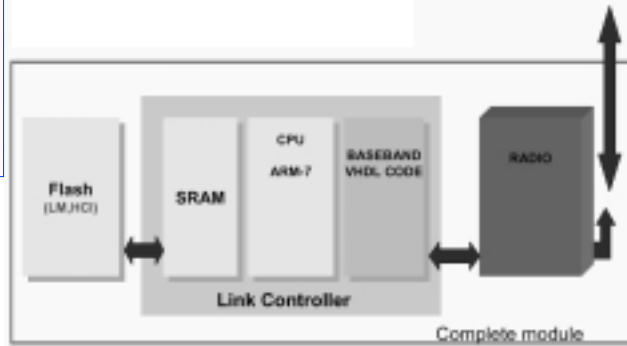
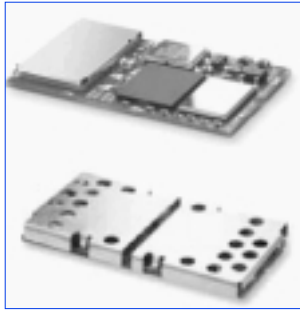
Hardware/Software Partitionierung

- Zeitaufwendige und/oder zeitkritische Prozeduren sollten in HW implementiert werden (Header Fehlerkorrektur, FEC, Verschlüsselung...).

Die 5-Chip Lösung



Die 3-Chip Lösung

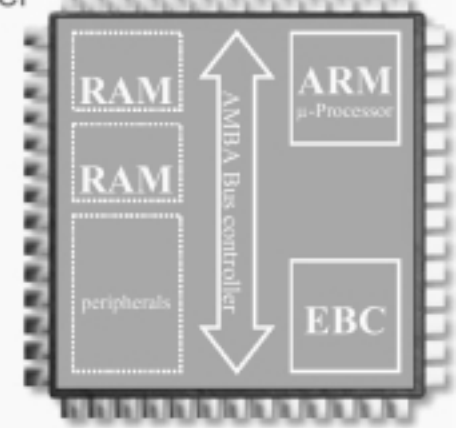


Die 3-Chip Lösung

The Link controller

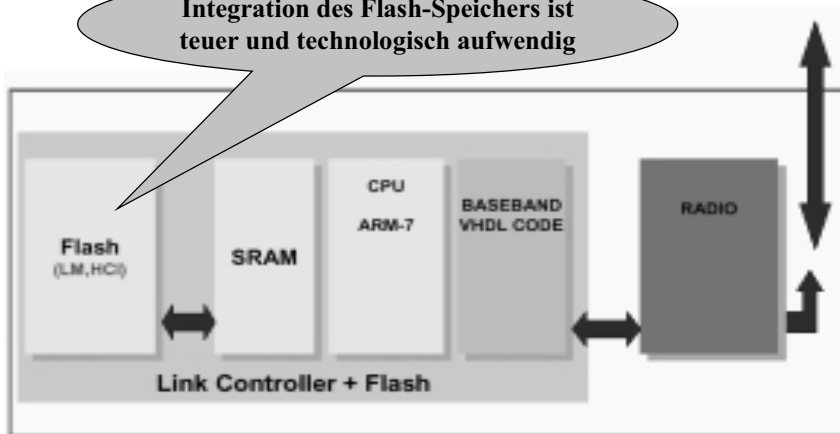
Features

- Baseband
- 3 UART's
- USB
- IRDA
- I2C
- PCM
- JTAG
- ARM-7 CPU



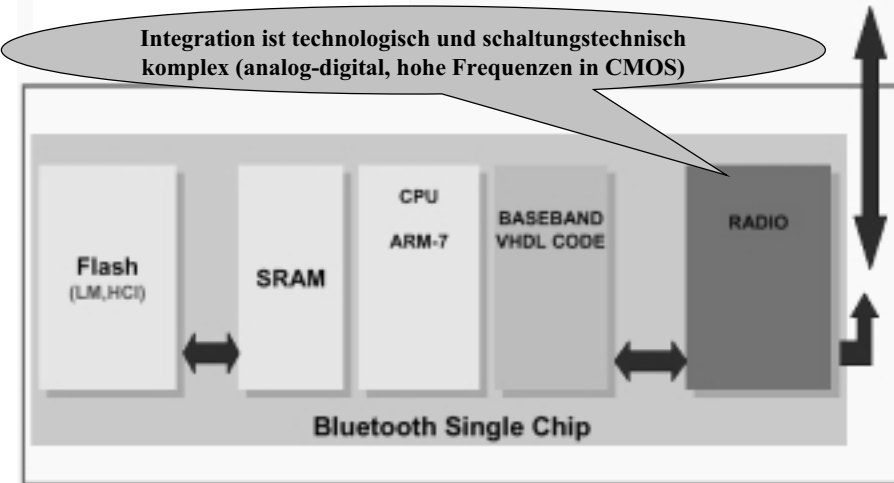
Die 2-Chip Lösung

Integration des Flash-Speichers ist teuer und technologisch aufwendig

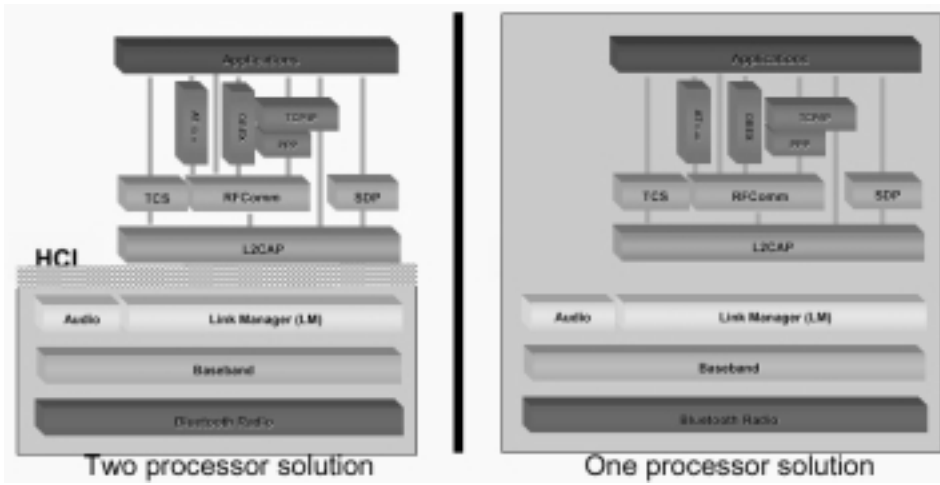


Die 1-Chip Lösung

Integration ist technologisch und schaltungstechnisch komplex (analog-digital, hohe Frequenzen in CMOS)

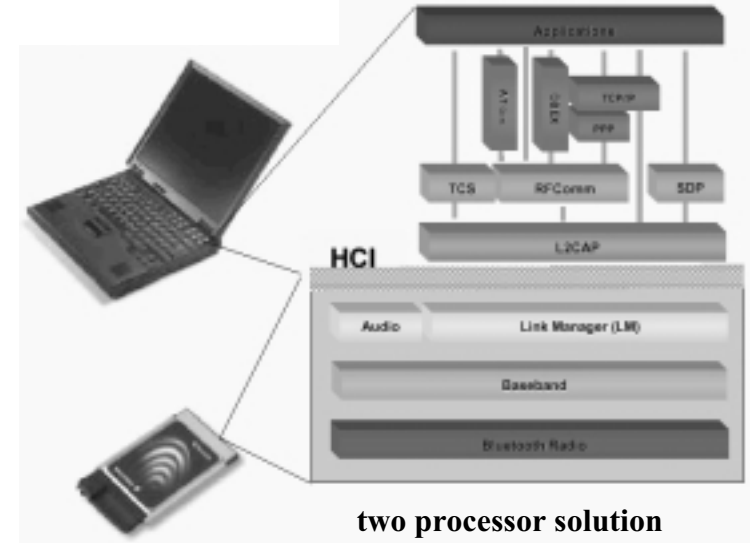


System-on-a-Chip



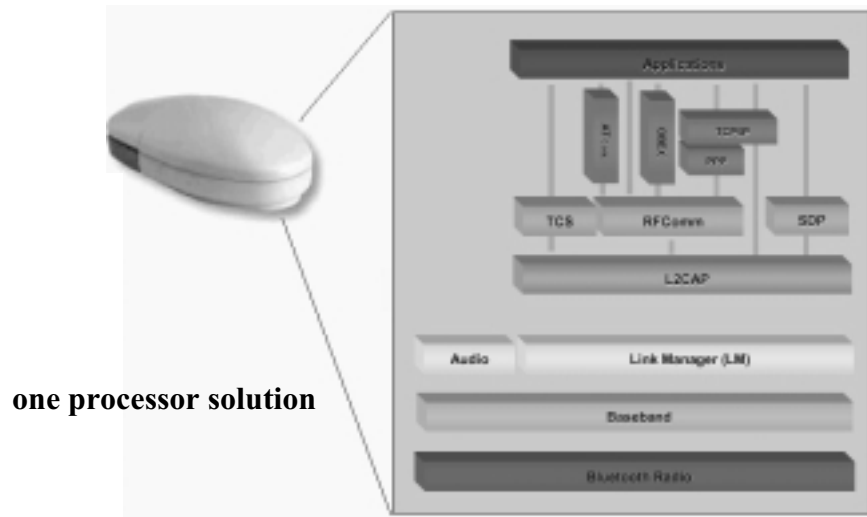
53

System-on-a-Chip



54

System-on-a-Chip



55